Identity Management In Cloud Computing

Mr. Chris Villemuer& Dr. Syed Adeel Ahmed

Abstract: *This paper discusses the adoption of cloud computing by many businesses and organizations. Cloud adoption has many benefits such as reduced IT costs, and accelerated adoption of new services. However, this accelerated adoption present challenges to effective Identity Management. Many existing Identity Management problems exist in cloud computing, but are further complicated. Now IT professionals must think outside the realm of the internal IT infrastructure to integrate cloud services into the organization. User provisioning/deprovisioning, credential management, auditing/access monitoring, and federal regulation compliance must be considered across the boundaries of the internal organization's network. Traditional Identity Management systems can be leveraged to solve these issues. Most cloud service providers have means to integrate on-premise Identity Management systems and identity records into their services. This requires bridiging and/or proxy systems for on-premise resources to interact with cloud services. Vendors such as Microsoft andCelestix provide such systems that bridge between on-premise and the cloud. New solutions are also being developed and adopted with a "cloud first" approach in the form of Identity as a Service (IDaaS). This is an evolving new approach that has potential to also revolutionize how Identity Management is conducted in organizations. Any solutions adopted to meet cloud Identity Management challenges must still comply with organizational and federal regulation requirements.*

Keywords: *Cloud, Identity Management, IDaaS, password sprawl, on- premise, auditing, compliance*

I. Introduction

The Information Technology industry has been embracing a new computing model in recent years. This model is known as cloud computing.Prior to this, many organizations administered to and operated their own physical IT infrastructures from within, also referred to as on-premise computing. Hosting resources on-premise has proven to be costly. Industry practices such as the "5 Year Rule" for replacing on-premise hardware continually drives up costs. The figure below is an example of the TCO(Total Cost of Ownership) to host an application on a physical server vs hosting on a virtual server in the Microsoft Windows Azure cloud. The TCO for on-premise hosting over 5 years is greater than hosting in Azure (Wlodarz, 2013).

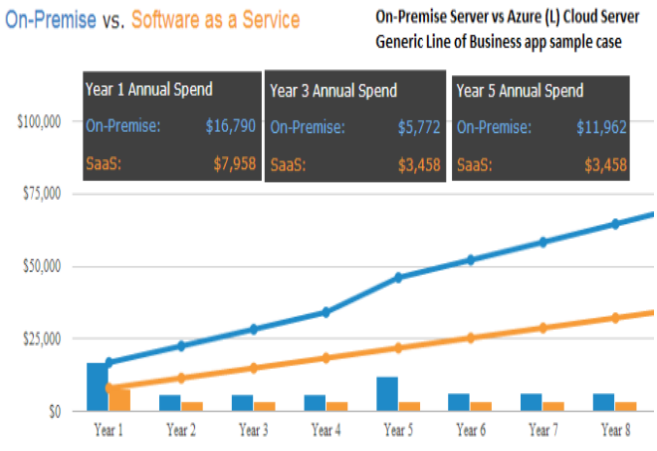

Figure 1.TCO generated from http://softwareadvice.com/tco/

To reduce these costs, organizations have been moving various IT roles and services to cloud platforms. While this approach has proven effective at reducing up-front costs such as hardware maintenance, it presents new challenges for enterprise Identity Management. Failing to meet these challenges can have higher costly results than the net savings gained from cloud adoption. There are solutions and approaches available to help organizations gain the benefits of cloud adoption while limiting risk and facing challenges associated with effective Identity Management in cloud computing.

II. Problem

Cloud platforms and services provide various benefits such as cost savings andmore rapid deployment of applications/service. However, Identity and Access Management for these entities remains a constant need. IT professionals within an organization are still responsible for facilitating user access to these new cloud services. In many cases, this facilitation requires on-premise processes and resources to interact with cloud providers. This results in an increased scope of Identity Management and security controls.

2.1. User Provisioning/Deprovisioning

At the core of Identity Management is provisioning identities/users within systems. This establishes "who am I" with a system's context. These established identities are then granted access to system components based on varying criteria such as

roles.IdM systems such as Microsoft Identity Manager 2016 or Oracle Identity Manager are responsible for provisioning and deprovisioning identities in various on-premise systems. Setup and on-going maintenance of these Identity and Access Management systems for on-premise services are traditionally costly. In many cases, custom logic is written into these systems to interact with specific on-premise systems. Unfortunately, many traditional IdM systems are not designed to operate outside of an enterprise firewall, or simply do not have adequate controls to interact with continually evolving cloud services (Musthaler, 2013). As a result, IT professionals must develop customized manual or partially automated processes to integrate cloud services into the IT infrastructure. These cloud services often have their own login systems and connector APIs that do not always work with internal/on-premiseIdM systems (Chickowski, 2013).

2.2. User Password Sprawl

Once an identity is provisioned in a cloud system, sufficient credentials must be established to leverage it. The user must present these credentials to authenticate access to a system. The most frequently used form of credential is a username and password combination. Many organizations must comply with federal laws and regulations for securely managing user credentials.

On-premise applications either have their own identity stores, or somehow leverage an existing identity store containing credentials. Cloud-based services often follow the same model. However, many organizations employ firewalls or other security controls to prevent external entities from accessing on-premise credentials. This presents an added challenge for integrating cloud services into existing IT infrastructures. A quick workaround to this problem is to simply provision a new identity and set of credentials in the cloud. More often than desired, organizations use this workaround to continue with rapid deployment of new cloud services.

The end result is a sprawl of username and password combinations across many cloud services with users having to track these identities. According to Centrify, a popular IT Enterprise IDaaS provider, this has led to users writing down passwords on sticky notes or other easily accessible forms. These practices by users often result in increased security risk for the organization, and dissatisfaction among the user experience. This additional layer of identity management also creates administrative overhead that can overwhelm help desk managers and IT administrators(Centrify, 2015).

2.3. Auditing and Compliance

Many organizations have an Information Security Policy document that employees must follow. This document defines security requirements for leveraging IT in an organization. The definitions are often derived from internal security requirements, and federal regulatory requirements such as Sarbanes Oxley and HIPAA. However, the existence alone of this document is not enough to reduce security risk. Users do not always comply with policies defined in these documents for various reasons such as lack of understanding, or willful disregard of the policies.

This demonstrates the need for IT security compliance and auditing. These are also important components of Identity Management. Once an identity is established within a system, its access into critical data must be monitored. Audit policies and practices within systems allow activities to be tied to an individual's usage. This reduces risks associated with fraud, theft, and other potential breaches of valuable information (Howarth, 2014).

Most on-premise systems allow IT administrators to have granular control and visibility into raw audit logging data. However, cloud services do not offer the same functionality. Two common reasons for this are technical limitations by the cloud provider that make it not possible to share this information, or unwillingness by cloud provider to share this information. In general, terms and conditions offered by even IDaaS cloud providers are not equivalent to features offered by on-premise environments (Bedell, 2012). The feature disconnect in other cloud services without Identity Management as a focus is likely to be even greater.

III. Solution

The most commonly used approach to dealing with Identity Management issues in the cloud is to leverage on-premise Identity Management infrastructure as much as possible. This is an intuitive approach, which is likely to have the least overall cost in the long term, due to reduced risk of managing separate identities and avoiding unnecessary investments in extraneousIdentity Management processes or systems.

There are also cloud-based solutions available that can integrate with on-premise systems, as well as operate primarily in the cloud.

3.1. SingleSign-On

Identity Federation/Single Sign-On (SSO) has become widely adopted among organizations in recent years. It allows organizations to share identity and access information without actually transmitting copies of identity records and/or passwords.

A widely used SSO system is Microsoft's Active

Directory Federation Services (ADFS). ADFS is included as a feature of the Windows Server operating system at no additional financial cost. It allowsorganizations to create federated trusts with SSO systems in other organizations. Many cloud providers, such as Microsoft's Office 365, have seamless integration into ADFS. ADFS allows organizations to use credentials in existing Active Directory and LDAP directories. Leveraging on-premise credentials reduces the risksassociated with duplicating usernames and passwords across multiple systems. It also allows rapid deprovisioning and access control for users in cloud applications and services(Chickowski, 2013). Furthermore, on-premise audit logging systems still retain much of desired visibility into user access since authentication events occur on-premise.

Companies such as Celestix provide tools to further enhance the native integration of ADFS and Office 365. Celestix Federated is a made-ready solution that allows seamless implementations of ADFS and integration into existing Identity Management infrastructure (Celestix, 2016).

3.2. Identity Synchronization & Proxy

Another approach is to establish proxy services between on-premise identities and cloud providers. While identity federation / SSO can be viewed as a cloud Identity Management proxy system, it is different because it is built on industry standards that were designed to meet needs beyond Identity Management for cloud systems. Some vendors today provide proprietary systems that are specifically designed to integrate on-premise identities with their own cloud services.

Microsoft provides a free identity proxy/synchronization system known as Azure Active Directory Connect. This tool is designed to synchronize on-premise Active Directory identities to Office 365 and Azure cloud services. It allows for user provisioning/deprovisioning, bi-directional password synchronization, and group filtering. While it is not security best practice to distribute user credentials to other systems, password synchronization does reduce the number of distinct passwords a user must track. Which in turn reduces the risk a user will carelessly write passwords down on sticky-notes or other unsecure media. Also, group filtering allows on-premiseaccess control to cloud based systems, as well as leveraging existing auditing infrastructure for compliance.

Centrify offers an on-premise proxy service called Centrify Cloud Connector. This allows integration of on-premise identities in Active Directory to CentrifyIDaaS. This integration behaves as a true proxy. Identity datais not required to be synchronized to the cloud(Centrify, 2015). This eliminates the risk associated with user credential sprawl as it fully leverages existing on-premise Identity Management infrastructure. CentrifyIDaaS then bridges these identities into cloud services such as Office 365, and Google Apps for Work.

3.3. Identity as a Service (IDaaS)

The most rapidly developing approach to managing identities in cloud computing is Identity as a Service. This solution has minimal to no interaction with on-premise Identity Management systems. In some cases, IDaaScan be the primary Identity Management system and/or provider for an organization. Identities are provisioned and managed in the cloud, then presented to on-premise resources as needed.

PingIdentity provides an IDaaS solution called PingOne Directory. Identities are provisioned and managed in the PingOne Directory, and are made available via PingIdentity's SSO services. PingIdentity integrates with many popular SaaS cloud service providers such as Office 365, Google Apps, Box, and Amazon Web Services(PingIdentity, 2016). The PingIdentity SSO service can then be leveraged by on-premise resources such as ADFS.

While IDaaS is an emerging technology with a significantly different model than on-premise Identity Management systems, it shows promise for managing identities in the cloud. Unlike traditional IdM systems, IDaaS systems are being designed with a "cloud first" mentality. Organizations must be cautious in adopting IDaaS, as thorough testing and evaluation should be performed to ensure the desired IDaaS cloud service meets IT operational, administrative, and security requirements for the organization.

IV. Conclusion

Many organizations will continue to adopt cloud computing at an accelerated rate. This adoption will revolutionize how IT and business operations are conducted. However, the need for effective Identity Management remains constant. Cloud platforms present new challenges to Identity Management such as working around firewalls, while also demonstrating the need to address classic challenges. Effective user provisioning/deprovisioning and credential management process are still needed. Organizations must continue to comply with federal regulations for auditing and access of sensitive data. Classic solutions can be adopted to address the Identity Management challenges of cloud computing. New approaches such as IDaaS also present opportunities to supplement and/or improve IT industry standards for Identity Management. In the end, organizations must decide which Identity Management approaches best meet business needs.

REFERENCES

[1.] Bedell, C. (2012, November). Understanding IDaaS: The benefits and risks of Identity as a Service. Retrieved from TechTargetSearchCloudSecurity: http://searchcloudsecurity.techtarget.com/feature/Understanding-IDaaS-The-benefits-and-risks-of-Identity-as-a-Service

[2.] Celestix. (2016). 5 Must-Know Benefits of Microsoft Active Directory Federation Services (ADFS). Retrieved from Celestix:http://www.celestix.com/5-must-know-benefits-of-microsoft-active-directory-federation-services-adfs/

[3.] Centrify. (2015, August 06). Stop Password Sprawl with App Single Sign-on via Active Directory. Retrieved from Centrify: https://www.centrify.com/media/1113447/whitepaper-stop-password-sprawl-en.pdf

[4.] Chickowski, E. (2013, October 25). Identity Management In The Cloud. Retrieved from InformationWeek DarkReading: http://www.darkreading.com/identity-management-in-the-cloud/d/d-id/1140751?

[5.] Howarth, F. (2014, April 17). Identity Management in the Cloud: Top Tips for Secure Identities. Retrieved from SecurityIntelligence: https://securityintelligence.com/identity-management-cloud-tips-secure-identities-iam/

[6.] Musthaler, L. (2013, January 18). Identity and access management as a cloud-based service eliminates time, pain and cost. Retrieved from Network World: http://www.networkworld.com/article/2163744/infrastructure-management/identity-and-access-management-as-a-cloud-based-service-eliminates-time-p.html

[7.] PingIdentity. (2016). PingOne Directory. Retrieved from PingIdentity: https://www.pingidentity.com/en/products/pingone/directory.html

[8.] Wlodarz, D. (2013, November 04). Comparing cloud vs on-premise? Six hidden costs people always forget about. Retrieved from Betanews: http://betanews.com/2013/11/04/comparing-cloud-vs-on-premise-six-hidden-costs-people-always-forget-about/